ELSEVIER

Journal of Pure and Applied Algebra 96 (1994) 215–223

JOURNAL OF PURE AND APPLIED ALGEBRA

# Monomial bases in the Steenrod algebra

Dan Arnon

*Department of Mathematics, The Hebrew University, Jerusalem, Israel*

Communicated by C.A. Weibel; Received 21 September 1992; Revised 1 March 1993

**Abstract**

The standard basis in the Steenrod Algebra $\mathscr{A}_2$ has a certain maximality property with respect to a left-hand lexicographic ordering on the formal monomials in the symbols $\{\mathrm{Sq}^n\}_{n=1}^{\infty}$. We look for bases with similar maximality and minimality properties with respect to this ordering and the related right-hand ordering. The minimal bases turn out to be compatible with the $\mathscr{A}_2^{(n)}$-filtration of $\mathscr{A}_2$. They also give rise to a large collection of related bases

The mod-2 Steenrod algebra $\mathscr{A}_2$ is the noncommutative algebra over $\mathbb{Z}/2$ generated by the symbols $\{\mathrm{Sq}^i\}_{i=1}^{\infty}$ subject to the Adem relations:

$$\mathrm{Sq}^a\mathrm{Sq}^b = \binom{b-1}{a}\mathrm{Sq}^{a+b} + \sum_{i=1}^{\lfloor a/2 \rfloor}\binom{b-1-i}{a-2i}\mathrm{Sq}^{a+b-i}\mathrm{Sq}^i, \quad a < 2b.$$

As a graded vector space over $\mathbb{Z}/2$, $\mathscr{A}_2$ is generated by the set of all monomials, of which a subset, the so-called "admissible monomials", forms a graded vector space basis for $\mathscr{A}_2$.

The admissible monomials are defined to be the monomials $\mathrm{Sq}^I = \mathrm{Sq}^{i_r}\mathrm{Sq}^{i_{r-1}}\cdots\mathrm{Sq}^{i_0}$ where the sequence $I = (i_r, \ldots, i_0)$ has the property $i_{k+1} \geq 2i_k$ for $0 \leq k < r$. Such a sequence is accordingly called an admissible sequence. The admissible monomials can also be defined in the following equivalent manner. Define a monomial $\mathrm{Sq}^{i_m}\cdots\mathrm{Sq}^{i_0}$ to be *smaller* than $\mathrm{Sq}^{j_n}\cdots\mathrm{Sq}^{j_0}$ if the sequence $(i_m, i_{m-1}, \ldots, i_0)$ is lexicographically smaller than $(j_n, j_{n-1}, \ldots, j_0)$ when read from left to right. Then the admissible monomials are those which cannot be expressed as combination of larger monomials. This point of view naturally leads to the following definition.

**Definition 1.** Let $F$ be the free (noncommutative) graded algebra over a field $k$ generated by the set of symbols $\{x_i\}_{i\in I}$, and assume that for any integer $N$ only a finite


*SSDI* 0022-4049(93)E0051-5

number of symbols have degrees smaller than $N$. Let $\leq$ be any linear ordering on the monomials in $F$, and let $U$ be a two-sided homogeneous ideal in $F$. A monomial $M$ is *maximal* (*minimal*) with respect to $(U, \leq)$ if $M$ is not equivalent, mod $U$, to a linear combination of monomials larger (smaller) than $M$ under $\leq$.

The following observation is immediate:

**Corollary 2.** *Given $F$, $U$ and $\leq$ as above, the set of maximal (minimal) monic monomials forms a vector space basis for $F/U$.*

**Definition 3.** On the set $\mathscr{S}$ of finite sequences of nonnegative integers we define the *left-hand lexicographic ordering* as follows. Let $I = (i_m, \ldots, i_0)$ and $J = (j_n, \ldots, j_0)$. Then $I \leq_L J$ if
- $I$ is empty, or
- $J$ is nonempty and $i_m < j_n$, or
- $J$ is nonempty, $i_m = j_n$ and $(i_{m-1}, \ldots, i_0) \leq_L (j_{n-1}, \ldots, j_0)$.

In a similar fashion we define the *right-hand lexicographic ordering*, denoted by $\leq_R$.

Similarly, for two sequences of positive integers $I, J$, define $\mathrm{Sq}^I \leq_L \mathrm{Sq}^J$ if $I \leq_L J$. For two polynomials $P = \sum M_i$ and $Q = \sum N_j$ define $P \leq_L Q$ if $M_i \leq_L N_j$ for all $i, j$. Extend the definition of $\leq_R$ in a similar fashion.

**Remark.** Notice that the order relation was defined on formal monomials and polynomials. It is not well defined in $\mathscr{A}_2$. To avoid confusion, monomials and polynomials will always be considered as elements of the free algebra generated by the symbols $\{\mathrm{Sq}^i\}_{i=0}^{\infty}$. Identities in $\mathscr{A}_2$ will be denoted by $\equiv$. However, a basis of monomials will always mean a basis in $\mathscr{A}_2$.

The standard basis, therefore, is the basis of maximal monomials with respect to the ideal generated by the Adem relations and the left-hand lexicographical ordering. It is natural to ask what happens if we replace "maximal" with "minimal" or "left" with "right".

**Definition 4.** The *basic $\xi$-monomials* are the monomials of the form

$$X_k^n = \mathrm{Sq}^{2^n}\mathrm{Sq}^{2^{n-1}}\cdots\mathrm{Sq}^{2^k},$$

The *basic $\zeta$-monomials* are the monomials of the form

$$Z_k^n = \mathrm{Sq}^{2^k}\mathrm{Sq}^{2^{k+1}}\cdots\mathrm{Sq}^{2^n}$$

**Theorem 5.** (A) *The basis of minimal monomials with respect to* $\leq_L$ *consists of the monomials of the form*

$$X_{k_0}^{n_0} X_{k_1}^{n_1} \cdots X_{k_r}^{n_r}$$

*such that the sequence* $(n_0, k_0), (n_1, k_1), \ldots, (n_r, k_r)$ *is strictly increasing with respect to left lexicographic ordering.*

(B) *The basic of minimal monomials with respect to* $\leq_R$ *consists of the monomials of the form*

$$Z_{k_r}^{n_r} Z_{k_{r-1}}^{n_{r-1}} \cdots Z_{k_0}^{n_0}$$

*such that the sequence* $(n_0, k_0), (n_1, k_1), \ldots, (n_r, k_r)$ *is strictly increasing with respect to left lexicographic ordering.*

(C) *The basis of maximal monomials with respect to* $\leq_R$ *consists of the monomials*

$$\mathrm{Sq}^{j_r} \mathrm{Sq}^{j_{r-1}} \cdots \mathrm{Sq}^{j_0}$$

*such that* (1) $j_{k+1} \leq 2j_k$, (2) $j_k$ *is divisible by* $2^k$.

To prove any of these cases it is enough to show that

(I) any monomial which is not of the required form is not maximal (or minimal),

(II) the number of the monomials of degree $k$ having the required form is equal to the dimension of $\mathscr{A}_2$ at that degree.

We first prove part (II) in all cases. Obviously, in cases (A) and (B) we have the same number of monomials in each degree so we can handle them as one case. Notice that the basic $\xi$-monomial $X_k^n$ has the same degree as the dual algebra element $\xi_{n+1-k}^{2^k}$. Each element in the dual algebra can be uniquely written as a square-free polynomial in $\{\xi_{n+1-k}^{2^k}\}_{n \geq k \geq 0}$. The monomials in case (A) are repetition-free products of basic $\xi$-monomials in a prescribed order. Since the dual algebra has the same dimension in each degree as the primal algebra, the result follows. As for case (C), there is a bijection between the standard basis monomials and the monomials in case (C) defined as follows:

**Definition 6.** Let $\mathscr{T} \subset \mathscr{S}$ be the subset of admissible sequences and let $\mathscr{T}' \subset \mathscr{S}$ be the subset of sequences of form (C). Define $\Delta : \mathscr{T} \to \mathscr{T}'$ as follows. For an admissible sequence $I = (i_r, i_{r-1}, \ldots, i_0)$, $\Delta(I) = (j_r, j_{r-1}, \ldots, j_0)$, where

$$j_k = 2^k \left( i_{r-k} - \sum_{l=0}^{r-k-1} \vdots \right).$$

Notice that $\sum j_k = \sum i_k$, so $\Lambda$ is degree preserving. Also notice that $j_0 = e(I)$, the excess of $I$. We have to check that the new sequence is indeed in $\mathscr{T}'$:

(1) $2j_k - j_{k+1} = 2^{k+1}(i_{r-k} - 2i_{r-k-1}) \geq 0$ so $j_{k+1} \leq 2j_k$.

(2) Obviously, $2^k$ divides $j_k$.

So the correspondence is well defined. The inverse correspondence is

$$i_k = 2^{-(r-k+1)}\left(2j_{r-k} + \sum_{l=r-k+1}^{r} j_l\right).$$

That establishes part (II) in all three cases.

We now prove part (I) for case (B). We start with a general monomial $M = \mathrm{Sq}^{i_1} \cdots \mathrm{Sq}^{i_r}$. If for some $k$, $i_k$ is not a power of 2, then $\mathrm{Sq}^{i_k}$ is decomposable, and so can be expressed as a polynomial in lower Squares. Substituting this polynomial for $\mathrm{Sq}^{i_k}$ in $M$ will reduce it with respect to both left and right lexicographic ordering. So we can assume $i_k = 2^{j_k}$. Observe that now $M$ will *not* be of the form required in case (B) if and only if at least one of the following happens:

(1) For some $k$, $j_{k+1} > j_k + 1$.

(2) The sequence $\mathrm{Sq}^{2^m} Z_k^n$ with $k < m < n$ appears in $M$.

(3) The sequence $Z_k^n Z_k^n$ appears in $M$.

To resolve the first case, use the following relation, which holds when $t > s + 1$:

$$\mathrm{Sq}^{2^s}\mathrm{Sq}^{2^t} \equiv \mathrm{Sq}^{2^t}\mathrm{Sq}^{2^s} + \mathrm{Sq}^{2^{s+1}}\mathrm{Sq}^{2^t - 2^s} + \sum_{i=0}^{s-1} \mathrm{Sq}^{2^t + 2^s - 2^i}\mathrm{Sq}^{2^i}.$$

Resolving the second case is more involved. First note that without loss of generality we can assume $n = m + 1$. We now reduce the monomial $\mathrm{Sq}^{2^m} Z_k^{m+1}$ in several steps. One can prove by descending induction of $k$ that $Z_k^m \equiv \mathrm{Sq}^{2^{m+1} - 2^k} + L$, where $L <_R \mathrm{Sq}^{2^m}$. This gives us

$$\mathrm{Sq}^{2^m} Z_k^{m+1} \equiv \mathrm{Sq}^{2^m} Z_k^m \mathrm{Sq}^{2^{m+1}} \equiv \mathrm{Sq}^{2^m}\mathrm{Sq}^{2^{m+1} - 2^k}\mathrm{Sq}^{2^{m+1}} + \mathrm{Sq}^{2^m} L\,\mathrm{Sq}^{2^{m+1}}.$$

The right-hand summand is already lexicographically lower than $\mathrm{Sq}^{2^m} Z_k^{m+1}$, so we only have to deal with the left hand summand. Now we use the Adem relation

$$\mathrm{Sq}^{2^m}\mathrm{Sq}^{2^{m+1} - 2^k} \equiv \mathrm{Sq}^{2^{m+1} + 2^m - 2^k} + L',$$

where $L' <_R \mathrm{Sq}^{2^m}$. Now we are left with the problem of reducing $\mathrm{Sq}^{2^{m+1} + 2^m - 2^k}\mathrm{Sq}^{2^{m+1}}$. We use an Adem relation again to get

$$\mathrm{Sq}^{2^{m+1} + 2^m - 2^k}\mathrm{Sq}^{2^{m+1}} \equiv \binom{2^{m+1} - 1}{2^{m+1} + 2^m - 2^k}\mathrm{Sq}^{2^{m+2} + 2^m - 2^k} + L'',$$

where $L'' \leq_R \mathrm{Sq}^{2^{m+2^{m-1}-2^{k-1}}} <_R \mathrm{Sq}^{2^{m+1}}$. Since the binomial coefficient in the left-hand summand is obviously zero, we are done.

To resolve the third case, we again use the identity $Z_k^n \equiv \mathrm{Sq}^{2^{n+1}-2^k} + L$, which gives

$$(Z_k^n)^2 \equiv LZ_k^n + \mathrm{Sq}^{2^{n+1}-2^k}L + (\mathrm{Sq}^{2^{n+1}-2^k})^2.$$

The first and second summands are lexicographically lower than $(Z_k^n)^2$. For the right-hand summand we use the Adem relation

$$(\mathrm{Sq}^{2^{n+1}-2^k})^2 \equiv \sum_{i=1}^{\lfloor 2^n-2^{k-1}\rfloor} c_i \mathrm{Sq}^{2^{n+2}-2^{k+1}-i}\mathrm{Sq}^i,$$

where the $c_i$ are some binomial coefficients. Since $i$ is bounded above by $2^n - 1$, we are done in this case as well, and so case (B) of the theorem is proved.

We now prove part (I) for case (A). Notice that by the same argument we used for case (B), the maximal monomials for case (A) must be comprised of power-2 Squares only. Case (A) now follows easily from case (B). Notice that the monomials of case (A) are mirror images of the monomials of case (B). Recall that the Steenrod algebra admits an antiautomorphism $\chi: \mathscr{A}_2 \to \mathscr{A}_2$. We use the following property of $\chi$,

$$\chi(\mathrm{Sq}^{2^n}) \equiv \mathrm{Sq}^{2^n} + L,$$

where $L$ is a polynomial in lower Squares. In particular, substituting $L$ for $\mathrm{Sq}^{2^n}$ in any monomial reduces it lexicographically with respect to both left and right orders. Given any monomial which is comprised of power-2 Squares and which is not of the form (A), use case (B) and two applications of $\chi$ to get an expression of that monomial in terms of lower ones.

To prove part (I) for case (C), we use the dual algebra and the cohomology of the Eilenberg–Mac Lane spaces $K(\mathbb{Z}/2, n)$[1]. In [1, p. 51] Mosher and Tangora define a function $\gamma: \mathscr{T} \to \mathscr{S}$ as follows

$$\gamma(j_r, j_{r-1}, \ldots, j_0) = (j_r - 2j_{r-1}, \ldots, j_1 - 2j_0, j_0)$$

and prove that

$$\langle \xi^{\gamma(J)}, \mathrm{Sq}^I \rangle = \begin{cases} 0 & l(I) < l(J), \\ 0 & l(I) = l(J) \text{ and } I <_R J, \\ 1 & I = J. \end{cases}$$

where $l(I)$ is the length of the sequence $I$. The proof is by induction, using the following lemma.

[1] A direct proof using Adem relations is possible but slightly unpleasant.

**Lemma 7.** *Let $I \in S$ and $J \in \mathscr{T}$ be sequences of length k, and let $I_k \in \mathscr{T}$ be the sequence $I_k = (2^{k-1}, 2^{k-2}, \ldots, 1)$. Then*

$$\langle \xi^{\gamma(J+I_k)}, \mathrm{Sq}^{(I+I_k)} \rangle = \langle \xi^{\gamma(J)}, \mathrm{Sq}^{I} \rangle,$$

Along the same lines one can prove the same result with $\mathrm{Sq}^I$ replaced by $\mathrm{Sq}^{\Delta(I)}$, since $\Delta(I + I_k) = \Delta(I) + I_k$. That establishes the fact that monomials of form (C) form a basis.

We now look at the action of basis (C) on $H^*(K(\mathbb{Z}/2, n); \mathbb{Z}/2)$. According to Serre, $H^*(K(\mathbb{Z}/2, n); \mathbb{Z}/2)$ is a graded polynomial algebra freely generated by the elements $\{\mathrm{Sq}^I \iota_n \mid I \in \mathscr{T}, e(I) < n\}$, where $\iota_n \in H^n(K(\mathbb{Z}/2, n); \mathbb{Z}/2)$ is the fundamental class (see [2]).

**Definition 8.** The *halving endomorphism* $D$ on the free algebra generated by the Squares is defined by setting $D(\mathrm{Sq}^{2n}) = \mathrm{Sq}^n$ and $D(\mathrm{Sq}^{2n+1}) = 0$ for $n \geq 0$. In fact it induces an endomorphism of $\mathscr{A}_2$. The two properties of $D$ which we will need are:
- For cohomology class $x$ and $W \in \mathscr{A}_2$, $W(x^2) = (D(W)x)^2$.
- For any basis-(C) monomial $\mathrm{Sq}^I \mathrm{Sq}^{i_0}$, $D(\mathrm{Sq}^I)$ is basis-(C) monomial.

**Lemma 9.** *$H^*(K(\mathbb{Z}/2, n); \mathbb{Z}/2)$ is a polynomial algebra on the set of generators $\{\mathrm{Sq}^I \iota_n \mid I \in \mathscr{T}', I <_R (n)\}$.*

**Proof.** The set $\{\mathrm{Sq}^I \iota_n \mid I \in \mathscr{T}'\}$ generates $H^*(K(\mathbb{Z}/2, n); \mathbb{Z}/2)$ because the monomials of form (C) are basis for $\mathscr{A}_2$. If $I \in \mathscr{T}'$ satisfies $I \geq_R (n+1)$, then $\mathrm{Sq}^I \iota_n = 0$, so these generators are redundant. If $(n+1) >_R I \geq_R (n)$ then $\mathrm{Sq}^I = W \mathrm{Sq}^{2^{k-1}n} \mathrm{Sq}^{2^{k-2}n} \cdots \mathrm{Sq}^n$ where $W <_R (2^k n)$. Then

$$\mathrm{Sq}^I \iota_n = W \iota_n^{2^k} = (D^k(W)\iota_n)^{2^k},$$

where $D$ is the halving endomorphism. Since $D^k(W)$ is a monomial of basis (C) and since $D^k(W) <_R (n)$, we have proved that the alleged set of generators does indeed generate $H^*(K(\mathbb{Z}/2, n); \mathbb{Z}/2)$. That this set of generators generates the polynomial algebra freely follows immediately from the fact that the map $\Delta$ gives a degree-preserving bijection,

$$\Delta : \{\mathrm{Sq}^I \mid I \in \mathscr{T}, e(I) < n\} \to \{\mathrm{Sq}^I \mid I \in \mathscr{T}', I <_R (n)\}. \qquad \square$$

We are now ready to prove part (I) for basis (C). Let $M = \mathrm{Sq}^{p_r} \cdots \mathrm{Sq}^{p_1} \mathrm{Sq}^{p}$ be any monomial, and let its expansion in basis (C) be

$$M \equiv L + \sum_{t \geq 0} W_t \mathrm{Sq}^{2^{t-1}p} \mathrm{Sq}^{2^{t-2}p} \cdots \mathrm{Sq}^{p},$$

where $L$, $\{W_t\}_{t\geq 0}$ are polynomials such that $L \geq_R \mathrm{Sq}^{p+1}$ and $W_t <_R \mathrm{Sq}^{2^t p}$. Notice that $W_0$ gives all the monomials in the expansion which are lower than $\mathrm{Sq}^p$.

Let $M' = \mathrm{Sq}^{p_r} \cdots \mathrm{Sq}^{p_1}$. Then

$$M\iota_p = M'\mathrm{Sq}^p \iota_p = M'(\iota_p)^2 = (D(M')\iota_p)^2,$$

$$M\iota_p = L\iota_p + \sum_{t\geq 0} W_t \mathrm{Sq}^{2^{t-1}p}\mathrm{Sq}^{2^{t-2}p}\cdots\mathrm{Sq}^p\iota_p = \sum_{t\geq 0}((D^t W_t)\iota_p)^{2^t}.$$

First consider the cases where either $M'$ contains an odd Square or $p_1 > 2p$. In the first case $D(M') = 0$ and we get $M\iota_p = 0$. In the second case we also get $M\iota_p = 0$. Therefore we have

$$\sum_{t\geq 0}((D^t W_t)\iota_p)^{2^t} = 0.$$

Notice that $D^t(W_t)$ is a sum of basis-(C) elements, all of which are lexicographically smaller than $\mathrm{Sq}^p$. Since those elements form a free polynomial basis when acting on $\iota_p$, the above polynomial equation gives $D^t(W_t) = 0$ for all $t$, and since all the Squares in $W_t$ have degrees divisible by $2^t$, we have $W_t = 0$ for all $t$. So $M \equiv L$ in this case, where $L \geq_R \mathrm{Sq}^{p+1}$ and therefore $L >_R M$.

In case $M'$ contains no odd Squares, we can assume by induction that $D(M') \equiv L'$ where $L' \geq_R D(M')$. Lifting this equation we get $M' \equiv L'' + N$ where $D(L'') = L'$ and all the monomials of $N$ contain odd Squares. Then

$$M = M'\mathrm{Sq}^p \equiv L''\mathrm{Sq}^p + N\mathrm{Sq}^p,$$

where $L''\mathrm{Sq}^p \geq_R M$ and $N\mathrm{Sq}^p$ can be made bigger than $M$ by the previous argument. Therefore the above equation provides an expression of $M$ as a sum of bigger monomials unless $L'' = M'$ and $N = 0$. In that case $D(M')$ must be a basis-(C) monomial, and therefore $M$ would also be a basis-(C) monomial unless $p_1 > 2p$. But that case has already been dealt with, and so $M$ is a basis-(C) monomial and we are done. □

We now look at some properties of bases (A) and (B). Recall that $\mathscr{A}_2^{(n)} \subset \mathscr{A}_2$ is the subalgebra generated by $\{\mathrm{Sq}^{2^t}\}_{t=0}^n$. This subalgebra is finite-dimensional, with $\dim(\mathscr{A}_2^{(n)}) = 2^{\binom{n+2}{2}}$ (see [1, pp. 56–57]). The intersection of basis A with $\mathscr{A}_2^{(n)}$ is made up of monomials composed of $\{X_k^m \mid m \leq n\}$. Constructing such a monomial amounts to choosing a subset of this collection of basic $\xi$-monomials, since the order in which they are multiplied is fixed. The size of the collection is $\binom{n+2}{2}$, and so we get the following proposition.

**Proposition 10.** *Bases* (A) *and* (B) *factor through* $\mathscr{A}_2^{(n)}$, *i.e., their intersections with* $\mathscr{A}_2^{(n)}$ *give vector space bases for this subalgebra.* □

Another interesting fact to note is that those bases bring out the symmetry of $\mathscr{A}_2^{(n)}$. Since the construction of a basis element in $\mathscr{A}_2^{(n)}$ amounts to a choice of a subset of the collection $\{X_k^m \mid m \leq n\}$ one can show the symmetry by passing to the complement. In particular, the top element of $\mathscr{A}_2^{(n)}$ is constructed by choosing the whole set, so it is equal to $X_0^0 X_0^1 X_1^1 X_0^2 X_1^2 \cdots X_n^n$ or other words to $\mathrm{Sq}^I$ for

$$I = (1, 2, 1, 2, 4, 2, 1, 4, 2, 4, 8, 4, 2, 1, 8, 4, 2, 8, 4, 8, \ldots, 2^n, 2^{n-1}, 2^n)$$

or

$$I = (2^n, 2^{n-1}, 2^n, \ldots, 8, 4, 8, 2, 4, 8, 1, 2, 4, 8, 4, 2, 4, 1, 2, 4, 2, 1, 2, 1).$$

Next we investigate the behavior of basis (A) with respect to the dual algebra. We do that in a more general context. First, use the symbol $X_k^n$ to denote the element $\xi_{n+1-k}^{2^k} \in \mathscr{A}_2^*$, in addition to its current interpretation in $\mathscr{A}_2$. This should not cause confusion since in every instance it will be clear how to interpret it. Now define $\preceq$ to be the following partial order on the symbols $\{X_k^n\}$:

$$X_k^n \preceq X_{k'}^{n'} \quad \text{if } n \leq n' \text{ and } k \leq k'.$$

We have the following theorem.

**Theorem 11.** *Let $\leq$ be any linear ordering on the symbols $\{X_k^n\}$ extending $\preceq$. Let $\leq_{\mathrm{L}}$ be the left lexicographical ordering induced by $\leq$. Then the monomials*

$$\{X_{k_1}^{n_1} X_{k_2}^{n_2} \cdots X_{k_r}^{n_r} \mid X_{k_1}^{n_1} < X_{k_2}^{n_2} < \cdots < X_{k_r}^{n_r}\}$$

*form a basis for $\mathscr{A}_2$. Furthermore, given monomials $M, N$ in that set, and interpreting $M$ in the dual algebra, one has*

$$\langle M, N \rangle = \begin{cases} 0 & N <_{\mathrm{L}} M, \\ 1 & N = M. \end{cases}$$

**Proof.** Assume $N \leq_{\mathrm{L}} M$. Write $M = X_{k_1}^{n_1} \cdots X_{k_r}^{n_r}$, $N = X_k^n N'$ and notice that the coproduct on $\mathscr{A}_2^*$ gives

$$\phi^*(X_q^p) = \sum_{i=q}^{p+1} X_i^p \otimes X_q^{i-1},$$

where $X_{p+1}^p$ is interpreted as 1. For $q \leq i \leq p$ we have $X_q^p \preceq X_i^p$ and so $X_q^p \leq X_i^p$. Therefore we have

$$\langle M, N \rangle = \langle \phi^*(X_{k_1}^{n_1}) \cdots \phi^*(X_{k_r}^{n_r}), X_k^n \otimes N' \rangle,$$

where $X_k^n$ is smaller than or equal to the left-hand parts in each of the coproducts. The form $\langle M, N\rangle$ will equal zero unless the degrees of some of those left-hand parts add up to the degree of $X_k^n$. Observe that the degrees in a set $\{X_{k_2}^{n_2} | X_{k_2}^{n_2} \geq X_k^n\}$ cannot add up to the degree of $X_k^n$ unless the set has a unique element, and this unique element is $X_k^n$. If that happens, then for some $j$, $X_{k_j}^{n_j} \leq X_k^n$, and since $N \leq_L M$ this is only possible if $j = 1$ and $(n_1, k_1) = (n, k)$. In that case, $M$ and $N$ start with the same basic $\xi$-monomial, and we proceed by induction. The claim that the above monomials form a basis now follows since those monomials form a basis when interpreted in the dual algebra. □

The same theorem holds if basic $\xi$-monomials are replaced by basic $\zeta$-monomials and the interpretation of $Z_k^n$ in the dual algebra is defined to be $\zeta_{n+1-k}^{2^k}$.

Haynes Miller challenged me to use those bases to prove the conjecture that $(\mathrm{Sq}^{2^n})^{2n+2} \equiv 0$. I failed, so instead I would like to suggest more conjectures:

**Conjecture 12.** $(\mathrm{Sq}^{2^n})^{2n+1} \equiv X_0^{n-1} X_0^n X_1^n X_2^n \cdots X_{n-1}^n X_n^n$.

**Conjecture 13.** $(X_k^n)^{n+k+2} \equiv 0$.

## Acknowledgement

I would like to thank Mike Hopkins, Haynes Miller and Frank Peterson for helpful discussions and suggestions, and Tao-Kai Lam for encouragement and some surprising insights.

## References

[1] R.E. Mosher and M.C. Tangora, Cohomology Operations and Applications in Homotopy Theory, New York, (Harper and Row, 1968).

[2] J.-P. Serre, Cohomologie modulo 2 des complexes d'Eilenberg–Mac Lane, Comment. Math. Helv. 27 (1953) 198–231.

[3] N. Steenrod and D.B.A. Epstein, Cohomology Operations, Annals of Mathematics Studies, Vol. 50 (Princeton University Press, Princeton, NJ, 1962).